CLAIMS

What is claimed is:

1. A method, comprising:

generating a first level trusted computing base (TCB) having a plurality of hardware components including a trusted platform module (TPM);

forming an extended TCB by adding a second level TCB to the first level TCB, wherein the second level TCB is software-based; and

transferring properties associated with the first level TCB to the second level TCB.

2. The method of claim 1, wherein the transferring of the properties is performed using a first level TCB interface having at least one of the following operations: secure storage, initiation of software integrity measurement, and attestation.

3. The method of claim 1, wherein the properties associated with the first level TCB comprise trust and security properties including at least one of the following: tamper-resistant secure storage, tamper-resistant software measurement, tamper-resistant attestation of previously measured values via tamper-resistant signature algorithms, and private keys.

4. The method of claim 1, further comprising:

adding one or more levels of software-based TCB to the extended TCB; and

transferring the properties associated with the first level TCB to the one or more levels of software-based TCB via one or more levels of TCB interfaces.

5. The method of claim 4, wherein a level of software-based TCB of the one or more levels of software-based TCB of a first system intact with a counterpart level of software TCB of a second system independent of other levels of the one or more levels of software-based TCB of the first system.

6. The method of claim 4, further comprising:

storing measured values depending on a level of abstraction of the one or more levels of software TCB; and

using the one or more levels of software TCB independent of hardware-based or software-based implementation of a level of software TCB below the one or more levels of software TCB.

7. The method of claim 1, wherein the second level TCB is executed independent of the first level TCB using a processor and main memory of a system.

8. The method of claim 1, wherein the second level TCB and the one or more levels of software-based TCB use encryption keys for attestation and secure storage, the encryption keys are encrypted using protected encryption keys in a TCB level below the second level TCB and the one or more levels of software-based TCB, certified via a signature of the private attestation key of the TCB level below the second level TCB and the one or more levels of software-based TCB, and stored in the TCB level below the second level TCB and the one or more levels of software-based TCB and terminating at the first level TCB being a root of trust for the extended TCB.

9. A method, comprising:

generating a first level trusted computing base (TCB) having a plurality of

hardware components including a trusted platform module (TPM);

forming an extended TCB by adding a second level TCB to the first level TCB, wherein the second level TCB is software-based;

adding a first virtual software TPM to the second level TCB; and

transferring properties associated with a hardware TPM of the first level TCB to the first virtual software TPM.

10. The method of claim 9, further comprises generating a first virtual container corresponding to the first virtual software TPM, the first virtual container comprises trusted services including at least one of the following: network services, file system services, and provisioning services.

11. The method of claim 9, further comprises:

adding one or more virtual software TPMs to the extended TCB, the one or more virtual software TPMs having the properties associated with the hardware TPM of the first level TCB; and

generating one or more virtual containers corresponding to the one or more virtual software TPMs, the one or more virtual containers comprise trusted applications including at least one of the following: login, biometric pattern matching, and protected signal processing.

12. The method of claim 10, wherein the first virtual software TPM comprises security assurance properties assigned to the first virtual containers to separate the first virtual containers from control of the hardware TPM.

13. The method of claim 10, wherein the first virtual software TPM comprises tamper-resistance properties derived from an address space isolation features and

integrity measurement capabilities exposed by the first level TCB.

14. The method of claim 9, further comprises transferring the properties associated with the hardware TPM of the first level TCB to the one or more virtual software TPMs, wherein the properties including the security assurance properties and the tamper-resistance properties.

15. The method of claim 9, wherein the first level TCB comprises a root of trust for the extended TCB including the first level TCB, the second level TCB, the first virtual software TPM, the one or more virtual software TPMs, the first virtual container, and the one or more virtual containers.

16. The method of claim 15, further comprising:

deleting data associated with the first virtual software TPM and the one or more virtual software TPMs of a first system to a counterpart virtual software TPM of a second system; and

seamlessly migrating the data associated with the first virtual software TPM and the one or more virtual software TPMs of a first system to a counterpart virtual software TPM of a second system.

17. An extended trusted computing base, comprising:

a first level trusted computing base (TCB) having a plurality of hardware components including a processor and a trusted platform module (TPM); and

one or more levels of TCB coupled with the first level TCB, wherein the one or more levels of TCB comprise one or more levels of software-based TCB having properties similar to trust and security properties associated with

the first level TCB.

18. The extended TCB of claim 17, further comprises a hardware secure storage facility coupled with the first level TCB and one or more virtual secure storage facilities coupled with each of the one or more levels of TCB.

19. The extended TCB of claim 17, wherein the plurality of hardware components comprises a chipset to couple the TPM with the processor.

20. The extended TCB of claim 17, wherein the one or more levels of TCB are generated by receiving the trust and security properties associated the first level TCB via one or more levels of TCB interfaces, the trust and security properties include at least one of the following: secure storage, tamper-resistant measurement, and attestation.

21. A system, comprising:

a storage medium;

an extended trusted computing base (TCB) coupled with the storage medium, the extended TCB having

a first level TCB having a plurality of hardware components including a processor and a trusted platform module (TPM), and

one or more levels of TCB coupled with the first level TCB, wherein the one or more levels of TCB comprise one or more levels of software-based TCB having properties similar to trust and security properties associated with the first level TCB; and

a hardware secure storage facility coupled with the first level TCB and one or more virtual secure storage facilities coupled with each of the one or more

levels of TCB.

22. The system of claim 21, wherein the one or more levels of TCB are generated by receiving the trust and security properties associated the first level TCB via one or more levels of TCB interfaces, the trust and security properties include at least one of the following: secure storage, tamper-resistant measurement, and attestation.

23. The system of claim 21, wherein the plurality of hardware components further comprises a chipset to couple the TPM with the processor.

24. A machine-readable medium having stored thereon data representing sets of instructions, the sets of instructions which, when executed by a machine, cause the machine to:

generate a first level trusted computing base (TCB) having a plurality of hardware components including a trusted platform module (TPM);

form an extended TCB by adding a second level TCB to the first level TCB, wherein the second level TCB is software-based; and

transfer properties associated with the first level TCB to the second level TCB.

25. The machine-readable medium of claim 24, wherein the properties associated with the first level TCB comprise trust and security properties including at least one of the following: tamper-resistant secure storage, tamper-resistant software measurement, tamper-resistant attestation of previously measured values via tamper-resistant signature algorithms, and private keys.

26. The machine-readable medium of claim 24, wherein the sets of instructions which, when executed by the machine, further cause the machine to:

add one or more levels of software-based TCB to the extended TCB; and

transfer the properties associated with the first level TCB to the one or more levels of software-based TCB via one or more levels of TCB interfaces.

27. The machine-readable medium of claim 24, wherein the second level TCB and the one or more levels of software-based TCB use encryption keys for attestation and secure storage, the encryption keys are encrypted using protected encryption keys in a TCB level below the second level TCB and the one or more levels of software-based TCB, certified via a signature of the private attestation key of the TCB level below the second level TCB and the one or more levels of software-based TCB, and stored in the TCB level below the second level TCB and the one or more levels of software-based TCB and terminating at the first level TCB being a root of trust for the extended TCB.

28. A machine-readable medium having stored thereon data representing sequences of instructions, the sequencing of instructions which, when executed by a machine, cause the machine to:

generate a first level trusted computing base (TCB) having a plurality of hardware components including a trusted platform module (TPM);

form an extended TCB by adding a second level TCB to the first level TCB, wherein the second level TCB is software-based;

add a first virtual software TPM to the second level TCB; and

transfer properties associated with a hardware TPM of the first level TCB to the first virtual software TPM.

29. The machine-readable medium of claim 28, wherein the sequences of instructions

which, when executed by the machine, further cause the machine to generate a first virtual container corresponding to the first virtual software TPM, the first virtual container comprises trusted services including at least one of the following: network services, file system services, and provisioning services.

30. The machine-readable medium of claim 27, wherein the sequences of instructions which, when executed by the machine, further cause the machine to:

add one or more virtual software TPMs to the extended TCB, the one or more virtual software TPMs having the properties associated with the hardware TPM of the first level TCB; and

generate one or more virtual containers corresponding to the one or more virtual software TPMs, the one or more virtual containers comprise trusted applications including at least one of the following: login, biometric pattern matching, and protected signal processing.